Chapter

7 TECHNOLOGY TRANSFER, EXPORT CONTROLS, AND INTERNATIONAL PROGRAMS SECURITY

INTRODUCTION

The U.S. Government (USG) transfers defense articles, services, and training to other governments and international organizations through both traditional Security Assistance (SA) programs and Security Cooperation (SC) programs. This chapter focuses on the technology and related controlled information associated with articles and services transferred under both SA and SC programs. This chapter will also address the broad spectrum of international programs security requirements.

As markets for military equipment continue to evolve, competition based on leading-edge technology has caused a significant increase in economic espionage aimed at U.S. technology. Although economic security is an important part of American foreign policy, military strength remains an essential instrument of foreign policy. It is Department of Defense (DoD) policy to treat defense-related technology as a valuable and limited national security resource. Determining which technologies should be controlled and to what extent necessitates an understanding of two seemingly conflicting elements of U.S. policy on international trade:

- Free trade—the importance of international trade to maintaining strong U.S. defense industrial base
- National security—the need to restrict the export of technology, goods, services, and munitions that would otherwise contribute to the military strength of countries that affect U.S. national security

Keeping in mind the balance between free trade and national security, it is the responsibility of those who control access to defense technologies to understand the laws, regulations, and directives that govern their international transfer. Traditional SA programs are mechanisms through which technology transfer may occur. International armaments cooperation programs with allies and friends are another means of transferring technology, especially through co-development, coproduction, and commercially licensed production programs.

Once technology transfer is discussed, and the methods used to transfer and control such exports have been covered, one still needs to know how to transfer technology by approved and secured means. Controlling the level of technology transferred to foreign governments and international organizations is a subset of the concept of international programs security (IPS). We should start off with a definition of an international program or activity and the security within such programs or activities:

- An international program is a lawful and authorized government or commercial effort in which there is a contributing or receiving foreign government or international participant, and information or technology is transferred from one entity to another.
- International programs security is the total effort to safeguard information and technology identified as requiring control generated by, provided to, or transferred within an international program or activity.

This chapter is organized into two main topics: 1. Technology Transfer and Export Control Policy and 2. International Programs Security Requirements (IPSR) with eleven sub topics:

1. Technology Transfer and Export Control Policy
    - Concept of technology transfer and export controls
    - Executive Branch key players for exports
    - Controlled Unclassified Information (CUI)
    - Foreign Disclosure and the National Disclosure Policy (NDP) (for classified items/ information)
    - Export Control Reform Initiative
    - Export approval and license process
2. International Programs Security Requirements
    - International visits and assignments
    - International transportation of classified military materiel
    - Role of Defense Security Service (DSS) in international programs
    - Foreign government and the North Atlantic Treaty Organization (NATO) information
    - Committee on Foreign Investment in the U.S. (CFIUS) and Foreign Ownership, Control, or Influence (FOCI)

Technology Transfer and Export Control Policy

The Concept of Technology Transfer and Export Controls

Technology transfer is the process of transferring, from government or industry in one country to another country, technical information relating to the design, engineering, manufacture, production, and use of goods and/or services. To comply with U.S. policy, technology transfer is regulated by a myriad of USG agencies, and is ultimately controlled by government-to-government agreements which can take the form of memoranda of understanding (MOUs), general security agreements (GSAs), letters of offer and acceptance (LOAs), export licenses, or other forms mutually agreed to by both governments or international governments. The *Security Assistance Management Manual* (SAMM), Chapter 3, "Technology Transfer and Disclosure," is a key reference when working technology transfer aspects of SC programs or activities.

It bears reiteration that the transfer policies addressed in this chapter apply primarily to defense technologies. The policy and controls discussed herein are not typically applied to common or "public domain" reference materials such as military standards, specifications, handbooks, or commercial counterparts to these documents. U.S. industry representatives may determine if their materiel is within public domain by submitting documents to the Office of the Assistant to the Secretary of Defense for Public Affairs.

Department of Defense Policy on Technology Transfer

The primary policy governing the process of technology transfer is contained in DoDI 2040.02, *International Transfers of Technology, Articles, and Services*. This instruction establishes DoD policy, assigns responsibilities, and prescribes procedures for the international transfer of dual-use and defense

related technology, articles, and services. It outlines working relationships among the Joint Staff, the Military Departments, and the various Defense Agencies. Selected U.S. technology laws and other appropriate DoD and military services directives are listed as references to this chapter.

DoDI 2040.02 states:

- Dual-use and defense-related technology will be treated as a valuable national security resource, to be protected and transferred only in accordance with export control laws and regulations, and national security and foreign policy objectives.
- In applying export control and technology security policies, emphasis will be given to preserving the U.S. military's technological superiority, establishing and maintaining interoperability with allies and coalition partners, and managing direct and indirect impacts on the defense industrial base.
- In recognition of the importance of international trade and scientific and technological cooperation, DoD must apply export control and other technology security policies and procedures in a way that takes into account support of the defense industrial base while maintaining U.S. nonproliferation imperatives.
- In determining DoD interests in technology and the means by which those interests are protected, DoD will consider such factors as the impact on the U.S. defense industrial base to support defense technologies, scientific and technological acceleration of change, as well as significant means in which scientific research and technological development are implemented in production.
- DoD will use available resources to achieve DoD and USG goals and objectives in transfers of technology, articles, and services, while recognizing that constant and rapid changes in technology pose difficult challenges in assessments, formulation of policy options, and implementation of policies.

Before we can understand how to control the transfer of technology, we must define a "defense article." Per the *International Traffic in Arms Regulations* (ITAR), Section 120.6, a "defense article" is any item or technical data designated in Section 121.1 of the ITAR, (i.e., the *U.S. Munitions List* (USML)). The USML identifies articles that have a primarily defense-related utility. So the USML addresses the "items," but what is "technical data?" Per the ITAR, Section 120.10:

> Technical data means: (1) Information, other than software as defined in Section 120.10(a)(4), which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation. (2) Classified information relating to defense articles and defense services on the USML and 600-series items controlled by the Commerce Control List.

The ITAR goes on to state at 120.10(b):

> This definition in paragraph (a) of this section does not include information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities, or information in the public domain as defined in §120.11 of this subchapter or telemetry data as defined in note 3 to Category XV(f) of part 121 of this subchapter. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles.

Technology Transfer Mechanisms

Within the context of SC, foreign military sales (FMS) and Direct Commercial Sales (DCS) are normally thought of as the primary means by which technology, goods, services, and munitions are transferred. However, as the following list (which is not all inclusive) illustrates, there are many different means for effecting transfers:

- Commercial and government sales
- Scientist, engineer, student, and academic exchanges
- Licensing and other data exchange agreements
- Co-development and coproduction agreements
- Commercial proposals and associated business visitors
- Trade fairs, exhibits, and air shows
- Sales to third-party nations
- Multinational corporation transfers
- International programs (such as fusion, space, and high energy)
- International meetings and symposia on advanced technology
- Patents
- Clandestine or illegal acquisition of military or dual-use technology or equipment
- Dissemination of technical reports and technical data, whether published, oral, or via oral/visual release
- Dissemination of technical reports under DoDD Manual 5400.07, *DoD Freedom of Information Act (FOIA) Program*
- Dummy corporations
- Acquiring an interest in U.S. industry, business, and other organizations

Basics of International Programs Security

To protect technologies being transferred, one must understand the legal and national policy basis for DoD's international programs and the principal security considerations to be taken prior to pursuing an international program. Three primary laws/regulations form the framework for NDP:

- Arms Export Control Act (AECA)
- Executive Order (E.O.) 13526
- National Security Decision Memorandum (NSDM) 119

Each of these will be covered in more detail below as will the associated "government-to-government" principle. Information for the remainder of this section comes primarily from the *International Programs Security Handbook* authorized by the Office of the Deputy Under Secretary of Defense (ODUSD) for Policy, the Defense Technology Security Administration (DTSA), February 1995 (Revised April 2010). An electronic version of the handbook can be found at http://www.discs.dsca.mil/_/pages/resources/default.aspx?section=publications&type=ips.

Access and Protection

U.S. law and policy requires that two fundamental considerations be addressed prior to sharing U.S. defense articles with a foreign government or international organization within international programs:

- U.S.'s Best Interest: Determining whether granting access to U.S. defense articles or information is in the best interest of the U.S.
- Adequate Protection: Determining whether the prospective recipient can and will satisfactorily protect the technology, article, or information.

In order to best understand these two fundamental security considerations, it may be useful to think of them as part of a formula. That formula is:

Best Interest of U.S. + Adequate Protection = Potential Access

Once the potential for access has been validated, actual export authorization of defense articles will be determined through further evaluation. Keep in mind that the considerations shown in the formula are specified by the AECA and will underpin everything discussed below.

Legal and Policy Basis for International Program Security

As alluded to above, the three principal documents providing the legal and national policy basis for security in most DoD international programs are the:

- AECA – Arms Export Control Act
- E.O. 13526 – Executive Order 13526
- NSDM 119 – National Security Decision Memorandum 119

Arms Export Control Act (AECA)

The AECA governs the export of defense articles and defense services to foreign countries and international organizations and includes both commercial and government programs. It authorizes a list of controlled articles, the USML, which is contained in the ITAR published by the Department of State (DoS) and is available online: https://www.pmddtc.state.gov/regulations_laws/itar.html. The AECA forms the legal basis for the security requirements in most DoD international programs. The AECA states that foreign sales (i.e., access) should be consistent with U.S. foreign policy interests, strengthen the security of the U.S., and contribute to world peace. The AECA also requires the President to provide Congress assurances that proposed recipient foreign countries or international organizations have agreed to certain security conditions regarding the protection of the articles or information. The three security-related conditions which must be satisfied prior to the export of controlled defense articles and information to a foreign country or international organization are:

- Transfer: The recipient country or organization agrees not to transfer title or possession of the articles or related technical data to anyone who is not an officer, employee or agent of the country or organization without prior USG consent
- Use: The recipient country or organization agrees not to use the articles or related technical data or permit their use for other than the purpose for which they were furnished without prior USG consent
- Protection: The recipient country or organization agrees to maintain security of the articles or related technical information, and provide substantially the same degree of security to it as does the USG

These security-related conditions are incorporated into the Foreign Military Sales (FMS) process via the standard terms and conditions of each Letter of Offer and Acceptance (LOA). Within any LOA, the standard terms and conditions will be listed at Section 2 "General Purchaser Agreements." Transfer, use, and protection are specifically addressed in subsections 2.4-2.6 of any LOA. By stating these conditions of sale in the LOA, the purchaser agrees to these conditions when they sign to accept the LOA. The specific language of these conditions may be found in Chapter 8 of this textbook.

Executive Order 13526

E.O. 13526, dated January 5, 2010 establishes the executive branch's classified National Security Information Program. Section 4.1 of this order states that access to classified information may be granted only when required in order to perform or assist in a lawful and authorized governmental function. This is the basis of the "need-to-know" principle. Further, persons authorized to disseminate classified information outside the executive branch shall assure the protection of the information in a manner equivalent to that provided within the executive branch. The executive order also states that classified information cannot be transferred to a third party without the consent of the originator. Additionally, it stipulates a requirement for the protection of any foreign government information (FGI) in the possession of the U.S. The executive order is implemented by *Classified National Security Information*, title 32 of the *Code of Federal Regulations* (CFR), part 2001 and 2003, effective 25 June 2010. The Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA), publishes "Classified National Security Information Directive 1" as the final rule pursuant to E.O. 13526 relating to classified national security information. It is also covered by DoD Manual 5200.01, *DoD Information Security Program*.

National Security Decision Memorandum (NSDM 119)

NSDM 119 provides the basic national policy governing decision-making on the disclosure of classified military information (CMI) to foreign governments and international organizations. NSDM 119 reiterates the basic requirements of the AECA and E.O. 13526, and emphasizes that CMI is a national asset, and that the USG will not share it with a foreign government or international organization (i.e., permit access) unless such a release will result in a clearly defined benefit to the U.S., and the recipient government or organization will provide substantially the same degree of protection.

Government-to-Government Principle

Classified information is shared with foreign governments and international organizations based on the government-to-government principle. This principle is defined by two activities relating to international programs. It applies to export and disclosure decisions, and to transfers of classified information and materiel:

- Decision: In keeping with the AECA, E.O. 13526, and NSDM 119, the decision concerns whether the USG will release classified information to another government or international organization.
- Transfer: If the decision above is in the affirmative, the actual transfer must be made either through official government-to-government channels (e.g., government courier) or through other channels approved by the responsible governments.

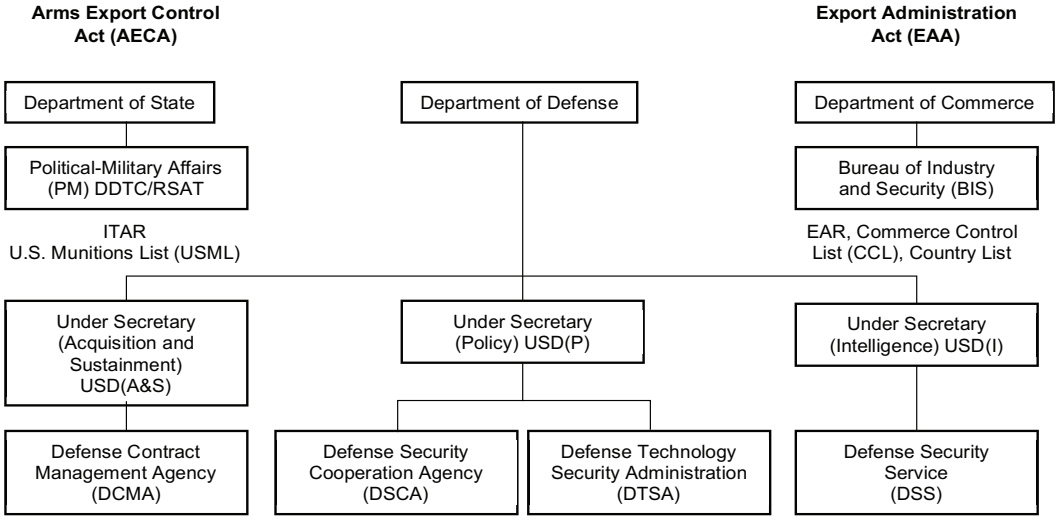
Transfer via government channels is necessary so that government accountability and control can be maintained from the point-of-origin to the ultimate destination. Transfers normally occur between Designated Government Representatives (DGRs) when custody is officially transferred to a recipient government or international organization. The recipient then assumes responsibility for the protection of the article or information. A security assurance must be obtained prior to transferring classified

material to a representative of a foreign government or international organization. A receipt must be obtained for classified information transfers to document the transfer of security responsibility.

Executive Branch Key Players for Exports

As covered in Chapter 2, Congress passes laws that govern how the USG functions. More specifically, certain laws or acts of Congress determine how the USG makes decisions for the export and import of military and dual-use items; dual-use meaning articles having both a military and civilian use. Two key laws, the AECA and the Export Administration Act (EAA), provide the legal authority for these type actions. As indicated in Figure 7-1, the Department of State (DoS) and the Department of Commerce (DoC) have the authority to implement these laws. DoD itself does not have any legal authority to approve the commercial export of defense items or information. The next sections in this chapter will discuss the authorities and organizational structures of the DoS, DoC, and DoD, and how these three departments work together to make decisions regarding export of military and dual-use items.

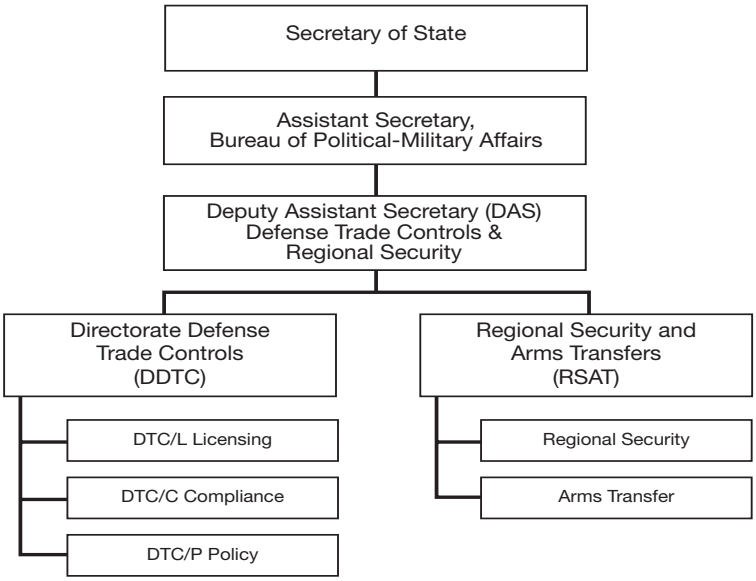
Figure 7-1
Key Players in Exports, Technology Transfer and International Programs Security



Department of State

Section 38, AECA, authorizes the President to control the import and export of defense articles and services, to designate such items as constituting the USML, and to promulgate implementing regulations. By E.O. 13637, the President has delegated his day-to-day responsibilities to the Secretary of State. The "implementing regulations" are the International Traffic in Arms Regulations (ITAR). The ITAR, 22 CFR parts 120-130, implements the AECA statutory authority to control the export of defense articles and services. By virtue of delegations of authority by the Secretary of State, these regulations are primarily administered by the Directorate of Defense Trade Controls (DDTC), which is under the Bureau of Political-Military Affairs, DoS. See Figure 7-2.

Figure 7-2
Department of State Export Authorization Structure



DTC/P has responsibility for updating and publishing the ITAR and the USML. The USML can be found in part 121 of the ITAR and is also discussed in SAMM, C3.3. The USML numerates articles, services, and related technical data as "defense articles" and "defense services" in accordance with Section 38, AECA. Those defense articles preceded by an asterisk (*) on the USML are designated significant military equipment (SME) that Section 120.7 of the ITAR defines as, "articles for which special export controls are warranted because of their capacity for substantial military utility or capability." Classified articles or information are always considered SME.

The USML is divided into twenty-one categories. An example is Category VII—Ground Vehicles. The categories are further divided into subtypes like Cat VII *(b) "Ground vehicles (not enumerated in the paragraph (a) of this category) and trailers that are armed or are specially designed to be used as a firing or launch platform..." (Note: the (*) before the (b) denotes everything listed in this subtype is SME.)

DTC/L is responsible for issuing export licenses for commercial sales of defense articles, services and technical data. They process on the order of 43,000 defense-related license requests yearly from U.S. contractors. Approximately 50 percent of these license requests are forwarded to DoD's Defense Technology Security Administration (DTSA) and the military departments (MILDEPs) for further review. DTSA will be discussed in greater detail when we cover DoD's role in exports. The DoS regulates permanent exports, temporary exports, and temporary imports of defense articles into the U.S., while the Department of Justice regulates permanent imports of defense articles (22 CFR parts 47, 178, and 179).

Another important office (shown in Figure 7-2) under DoS, Bureau of Political-Military Affairs, is the Regional Security Arms Transfer (RSAT) Office. While DDTC processes license requests from contractors for commercial sales, RSAT processes DoD requests for exports through FMS and the Letters of Offer and Acceptance (LOA)s. This is a key step in the process of developing and approving the LOA before it is offered.

Working through the DoS to get a license for every item that may be part of a larger military article slows down the export process and is very frustrating for the U.S. company trying to sell and export

and to the country waiting for the item. One of the "reforms" in the USG Export Control Reform Initiative is to move as many military items as possible from the DoS USML to the DoC Commerce Control List (CCL). This task started under President Obama's administration and is continuing today. By October 2013, many items once listed in the ITAR's USML had started to move to the CCL. Between Oct 2013 and Dec 2014, items listed in 15 of the 21 USML categories had items move to the CCL. The final items were scheduled to move by 2017. The goal is to eventually have just one list of military items with only truly "key" defense materiel listed as "controlled." A term used to describe this approach is "smaller but taller walls." This means the USG intends to eventually list fewer military items on the USML (i.e., smaller walls) while still listing on the USML the most important items and technologies which require the highest levels of protection (i.e., taller walls). The concept of a single export list is addressed later in this chapter under "Export Control Reform Initiative."

Department of Commerce

Under the Export Administration Act of 1979 (EAA), the DoC has licensing jurisdiction over all commodities and unclassified technical data except for certain specified items controlled by other government agencies, such as USML items controlled by the DoS, or atomic energy material controlled by the U.S. Department of Energy. The EAA applies to the following:

- Exports of commodities and technical data from the U.S.
- Re-exports of U.S.-origin commodities and technical data from foreign destinations
- U.S.-origin parts and components used in a foreign country to manufacture a foreign end product for export and in some instances, a foreign product produced as a direct product of U.S.-origin technical data

The *Export Administration Regulations* (EAR) (15 CFR Parts 368 through 399) issued by the DoC, Bureau of Industry and Security (BIS), prescribe licensing procedures for items under its jurisdiction. Controls on granting export licenses are based on considerations of national security, the fostering of U.S. policy and international responsibilities, the necessity for protecting the domestic economy from an excessive drain of scarce materials, and the reduction of the serious inflationary impact of abnormal foreign demand. Items controlled by the DoC for export are listed on the *Commerce Control List* (CCL). The list is very detailed and identifies items that may be exported to a given country. The DoC and BIS home page is at http://www.bis.doc.gov.

Dual-use items are items that were primarily designed for a civil application but which may have a potential military application (i.e., computers, utility vehicles, trucks, light aircraft, and global positioning systems, etc.). The DoC is charged with coordinating export requests for such items that fall into this category of dual-use. There are times when there is a question of whether an item is dual-use or specifically a military item. The DoS, DoD and DoC resolve such questions using what the ITAR Section 120.4 terms the "Commodity Jurisdiction (CJ)"process. A CJ determination form is sent to DoS. After consultation with DoD, DoC and other USG agencies, the DoS will make a determination if an item is primarily a military item or dual-use and thus who has jurisdiction, DoS or DoC.

The previous section covering the DoS introduced the ongoing Export Control Reform Initiative (ECRI), and recounted that many military items listed on the USML are now being administratively moved to the CCL. The CCL had already existed, but under the ECRI, the "600 Series" has been added to the CCL. The 600 Series is comprised of military items that were formerly listed in the DoS USML under the export authority of DDTC. These items are being moved to the CCL, under the Bureau of Industry and Security (BIS). The CCL's 600 Series differentiates those items that are, "critical to maintaining a military or intelligence advantage to the U.S.," from those that need less control like sewing machines or lawn mowers. The BIS added ten new 600 Series Export Control Classification Numbers (ECCNs) to the CCL to define these newly transferred items. Even though the items are still

controlled for export, the associated controls are much less stringent than those previously applied under the USML. More information about export reform is in the "Export Control Reform Initiative" section later in this chapter.

Department of Defense

Figure 7-1 provides an overview of the key players within the executive branch for technology transfer and international programs security. The Under Secretary of Defense for Policy (USD (P)) is responsible for international security matters. DTSA's International Security Directorate (ISD) is responsible for implementing NDP-1. More specifically, DTSA/ISD is the Executive Secretariat to the interagency National Military Information Disclosure Policy Committee (NDPC), the Designated Security Authority to develop NATO security policy for the USG, responsible for developing security policies and arrangements for international programs, and developing and negotiating international security agreements. Additionally, other DTSA Directorates (i.e., Licensing, Policy, and Technology) are the focal points for the development and implementation of DoD policy positions on matters concerning export control, including, but not limited to: the *International Traffic in Arms Regulations*, the *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*, the *Missile Technology Control Regime*, the *Export Administration Regulations*, etc. For example, when the DoS or DoC requires DoD input to decide if a license for export should be approved, the request goes to DTSA's Licensing Directorate to initiate the review process. DTSA's responsibilities will be covered in further detail under the topic of "exports" later in this chapter.

The Under Secretary of Defense for Intelligence (USD(I)) is responsible for DoD counterintelligence, security, intelligence programs, staff supervision of the Defense Security Service (DSS), and for publication of the *National Industrial Security Program Operating Manual* (NISPOM). All of these responsibilities, including security support for program protection planning, have applications to DoD acquisition programs. With the DSS field offices, USD(I) ensures that companies that manufacture military items adhere to the same laws and regulations concerning technology transfer as do individuals working for the USG.

The Under Secretary of Defense for Acquisition and Sustainment (USD (A&S)) is responsible for defense procurement and international armaments cooperation programs. These functions are performed by the Director, Defense Procurement and the Director, International Cooperation. The Defense Contract Management Agency (DCMA) also reports to USD (A&S). In addition to its normal management of DoD contracts, DCMA provides industrial security support at those defense contractor facilities where a DSS representative is not available.

The Joint Staff provides support that includes conducting operational and military mission impact assessments on technology, goods, services, and munitions transfer issues, as requested.

The Defense Intelligence Agency (DIA) performs the following functions in the support of U.S. defense technology security:

- Provides assessments of the types and numbers of illegal transfers of technology, goods, services, and munitions, and the associated transfer mechanisms
- Designates a point of contact to represent DIA on technology transfer matters
- Conducts end user checks and intelligence review on technology, goods, services, and munitions transfer cases
- Assesses foreign availability of technology, goods, services, and munitions proposed for transfer
- Provides intelligence concerning the total effect of transfers of technology, goods, services,

and munitions on U.S. security

- Provides intelligence expertise in interagency, national, and international fora on technology, goods, services, and munitions transfer matters
- Assists in identifying and assessing critical technologies

The DoD export control responsibilities and participating organizations are further depicted in Table 7-1.

Table 7-1
Department of Defense Organizational Export Control Responsibilities

Organization	Responsibility
USD (P)	Policy oversight
USD (A&S)	Technical oversight for national security and nonproliferation
DTSA	Coordinates reviews of export licenses
Joint Staff	Strategic rationale and validation
Intelligence community	Threat assessments of foreign nations
Military departments	Provide experts from defense labs and commands
Institute for Defense Analysis	Federally-funded R&D center providing DoD with technical support and economic security assessments
Industry and academia	Participate in technical working groups and multilateral negotiation

Controlled Unclassified Information

Controlled unclassified information (CUI) is a term used to collectively describe all unclassified information to which access or distribution limitations have been applied in accordance with applicable national laws or regulations and Volume 4 of DoDM 5200.01. A commonly seen marking for CUI in the U.S. is "For Official Use Only" (FOUO). FOUO information is unclassified official government information that has been determined by designated officials to be exempt from public disclosure under the Freedom of Information Act (FOIA). FOIA is designed to make government information available to the public and thus requires openness in government. It is not designed to protect information. It provides that the public is entitled to access to agency records, unless the record is exempt from disclosure. Government agencies apply their own unique markings to identify the information. Consequently DoD has several policy directives addressing the release of CUI. These documents are listed as references to this chapter:

- DoDD 5230.09 contains policies and procedures for the release of information for publication or public release
- DoDI 5200.21, and DoDD 5230.24 govern the release of DoD technical information
- DoDM 5400.07 contains the DoD policies and procedures governing FOIA requests
- DoDD 5230.25 provides procedures for the dissemination and withholding of unclassified technical data

On 9 May 2008, President Bush signed a memorandum for the heads of executive departments and agencies on the subject of "Designation and Sharing of Controlled Unclassified Information (CUI)." The memorandum states the following:

. . . adopts, defines, and institutes "Controlled Unclassified Information" (CUI) as

> the single, categorical designation henceforth throughout the executive branch for all information within the scope of that definition, which includes most information heretofore referred to as "Sensitive But Unclassified" (SBU) in the Information Sharing Environment (ISE), and establishes a corresponding new CUI Framework for designating, marking, safeguarding, and disseminating information designated as CUI.

Implementation of new CUI procedures is expected to take several years.

27 May 2009, President Obama signed a memorandum for the heads of executive departments and agencies with a subject of "Classified Information and Controlled Unclassified Information." In it, President Obama states:

> [M]y Administration is committed to operating with an unprecedented level of openness. While the Government must be able to prevent the public disclosure of information where such disclosure would compromise the privacy of American citizens, national security, or other legitimate interests, a democratic government accountable to the people must be as transparent as possible and must not withhold information for self-serving reasons or simply to avoid embarrassment.

This initiative may result in major changes as to how CUI is handled and disseminated. It will take years to implement all the changes, but U.S. officials dealing with foreign counterparts must be aware of the evolution of these policy changes.

Freedom of Information Act

Congress has stated the U.S. public generally has the right to know what its government is doing. The FOIA requires government information to be made available to the public unless the information falls within one of nine exemption categories described and the appropriate USG official determines the information should be withheld from disclosure. Only information falling into one of these categories may be marked FOUO:

- Exemption 1 is classified information. The FOIA permits the withholding of any information properly and lawfully classified under the provisions of E.O. 13526. The other eight exemption categories deal with unclassified but generally sensitive information.
- Exemption 2 permits the withholding of information that pertains solely to the internal rules and practices of a government agency.
- Exemption 3 permits the withholding of information that a statute specifically exempts from disclosure by terms that permit no discretion on the issue, or in accordance with criteria established by that statute for withholding or referring to particular types of matters to be withheld.
- Exemption 4 permits withholding information such as trade secrets and commercial and financial information obtained from a company on a privileged or confidential basis, which, if released, would result in competitive harm to the company.
- Exemption 5 protects inter- and intra-agency memoranda that are deliberative in nature.
- Exemption 6 provides for the withholding of information, the release of which could reasonably be expected to constitute a clearly unwarranted invasion of personal privacy of individuals.
- Exemption 7 permits withholding records or information compiled for law enforcement

purposes that could reasonably be expected to interfere with law enforcement proceedings; would deprive a person of the right to a fair trial or impartial adjudication; could reasonably be expected to constitute an unwarranted invasion of personal privacy of others; disclose the identity of a confidential source; disclose investigative techniques; or could reasonably be expected to endanger the life or physical safety of any individual.

- Exemption 8 permits withholding records or information contained in or relating to examination, operation or condition reports prepared by, on behalf of, or for the use of any agency responsible for the regulation or supervision of financial institutions.
- Exemption 9 permits withholding records or information containing geological and geophysical information and data (including maps) concerning wells.

It is DoD policy to place distribution statements on documents containing unclassified scientific and technical information produced either within DoD or on its behalf by others. This policy was only marginally directed toward restricting the disclosure of such information to the public and thus to foreign persons. Although it was the policy to apply such distribution markings, the practice did not always conform to the policy. The result was that sensitive scientific and technical information occasionally found its way into the public domain, including the foreign public. This potential loophole was resolved by Public Law 98-94, enacted 24 September 1983, which provided the Secretary of Defense with the authority to withhold from the public critical technologies under Exemption 3 of the FOIA. For more specific information on FOIA as it relates to LOAs and FMS procurement contracts, refer to SAMM, Section C3.5, "Release of Information."

Foreign Disclosure and the National Disclosure Policy (NDP)

The NDP was established as a framework for the approval or denial of the transfer of classified military information (CMI) to foreign governments and international organizations. CMI is defined as classified information that has been developed by or for the DoD, or is under the DoD's jurisdiction or control. Basic authority and policy for transferring classified information are contained in NSDM 119, which is implemented by the classified publication, *National Policy and Procedures for Disclosure of Classified Military Information to Foreign Governments and International Organizations*, short title NDP-1.

Effective implementation of NDP-1 is the responsibility of the USD (P). Disclosure officials are authorized, but not automatically obliged, to disclose information up to the classification levels indicated in the NDP-1 Annex for each category of information. Most importantly, each disclosure decision is made on a case-by-case basis.

National Disclosure Policy Committee/Exceptions to National Disclosure Policy

The NSDM 119, NDP-1, and DoDD 5230.11 *Disclosure of Classified Military Information to Foreign Governments and International Organizations* requires the establishment of an interagency NDPC, to formulate, administer, and monitor NDP. General members of the NDPC include:

- Secretary of State
- Secretary of Defense (appoints Chairman)
- Secretary of the Army
- Secretary of the Navy
- Secretary of the Air Force
- Chairman, Joint Chiefs of Staff

On a day-to-day basis, these officials are represented in NDPC decisions by designated senior officials on their staff. NDPC general members have a broad interest in all committee activities and vote on all issues that come before the committee. Other members (such as the Director of National Intelligence, the Secretary of Energy, and many others) may vote on issues in which they have a direct interest (see Attachment 7-1 for a list of all the members of the NDPC). When an exception to NDP (ENDP) is required, because disclosure criteria cannot be met within the existing authorized classification level, such exceptions may be granted only by the NDPC, the Secretary of Defense, or the Deputy Secretary of Defense. A request for an ENDP must be sponsored by a NDPC member, normally the cognizant MILDEP for the classified information proposed for transfer. For military weapon systems, this is normally the MILDEP that has developed and produced the system.

On February 14, 2017, the Secretary of Defense codified in NDP-1, the Military Intelligence Disclosure Policy Committee (MIDPC), The MIDPC is the central authority for the formulation, promulgation, administration, and monitoring of NDP-1 as it relates specifically to Category 8 (Military Intelligence). The MIDPC operates similar to the NDPC with a similar structure (see Attachment 7-2 for a list of all the members of the MIDPC). In situations where an ENDP includes multiple categories, to include Category 8, the NDPC has purview.

The NDP-1 Annex (classified) identifies the maximum classification level of information that can be released by country and by category of classified military information. NDP-1, by itself, does not authorize any disclosures. The Secretaries of the MILDEPs have generally been delegated authority by the NDP-1 to decide if CMI under their control may be released. The policy and guidance for implementing NDP-1 is contained in the DoDD 5230.11. This directive states that the MILDEPs will release CMI in accordance with the NDP-1 Annex only if all of the following five conditions or criteria, originally outlined in NSDM 119, are met:

1. Disclosure is consistent with U.S. foreign policy and national security objectives.

2. Disclosures, if compromised, will not constitute an unreasonable risk to the U.S. position in military technology or operational capabilities.

3. The foreign recipient of the information will afford it substantially the same degree of security protection given to it by the U.S. The intent of a foreign government to protect U.S. CMI is established in part by the negotiation of general security agreements.

4. Disclosure will result in benefits to the U.S. at least equivalent to the value of the information disclosed.

5. The disclosure is limited to information necessary to accomplish the purpose for which disclosure was authorized.

If the classification of the information proposed for disclosure exceeds the country's eligibility in the NDP-1 Annex, or if the policy criteria cannot be met, then the proposed disclosure must be denied or an ENDP must be approved by the NDPC or MIDPC. Moreover, even if the U.S. disclosure official has determined that eligibility in the NDP-1 Annex exists and that all policy criteria have been met, disclosures of CMI may not be made until the affected originator's approval has been obtained or appropriate authority to disclose has been received.

All disclosure authority rests in the first instance with the head of the department or agency which originates the information. In addition, all disclosure officials must be certain that they possess the required authority to disclose the information in question. The Secretary of Defense and the Deputy Secretary of Defense are the only officials who may grant unilateral exceptions to the NDP. The Secretary or Deputy Secretary of State, with the consent of the originating or responsible NDPC or

MIDPC member department or agency, may also authorize such disclosures. Under DoD Directive 5230.11, the Secretary of Defense has delegated disclosure authority to the secretaries of the MILDEPs and other DoD officials whose decisions must be in compliance with NDP-1. They are required to appoint a principal disclosure authority at component headquarters level to oversee the disclosure process and a designated disclosure authority at subordinate commands. SAMM, Section C3.2, "Disclosure of Classified Military Information," provides additional information on the national disclosure process as it relates to SC.

Security Surveys

In addition to making determinations on the release of CMI, the NDPC also conducts security surveys (also called security visits) of foreign governments or international organizations. NDPC teams conduct periodic visits to foreign governments and their national industrial bases to assess capability and intent to protect U.S.-origin CMI. The teams are usually made up of members of the DoS and DoD. The primary areas reviewed by the teams are personnel security, information security, industrial security and physical security. The views of the local U.S. embassy are also sought. If the result of a survey is satisfactory, it may result in an international security agreement (see below) with the other government. A survey may also result in changes to the classified annex in NDP-1 concerning a country's classification and eligibility for CMI without engaging the ENDP process.

International Security Agreements

E.O. 13526 requires persons authorized to disseminate classified information outside the executive branch shall ensure the protection of the information in a manner equivalent to that provided within the executive branch. In situations where classified information is being made available to foreign governments, these assurances may be obtained in several ways. First, they are included in the standard terms and conditions of FMS LOA, Section 2, "Conditions–General Purchaser Agreements." See Chapter 8 for further information. They may also be the subject of diplomatic notes, memoranda of understanding (MOUs) and similar correspondence. Separate international agreements known as General Security of Information Agreements (GSOIAs) or General Security of Military Information Agreements (GSOMIAs) have been concluded with approximately 72 countries. Since these are reciprocal agreements, the other governments may also send teams to the U.S. to ensure compliance with the agreements. GSOIA/GSOMIAs typically include the following topics:

- Protection, third-party transfer, and intellectual property rights provisions
- Classified information transfer mechanism (government-to-government)
- Definition of classified information
- Reciprocal provision for security expert visits
- Requirements for investigations in case of compromise
- Industrial security procedures
- Visit request procedures
- Limitations on level of classification

Disclosure Planning

DoD Directive 5230.11 requires that planning for possible foreign involvement should start at the beginning of the weapon system acquisition process to facilitate decisions on disclosure in support of foreign sales or cooperative programs. Chapter 13 of this textbook contains additional information.

Similarly, DSCA Policy 16-26 observes that foreign partners' procurement laws sometimes forbid the submission of a Letter of Request (LOR) for U.S. defense systems prior to a competition among several vendors. The lack of an LOR may impede timely initiation of U.S. Government technology release and foreign disclosure processes. In order to accelerate (when possible) the release reviews of U.S. technologies and to initiate foreign disclosure processes in the absence of an LOR, SCOs should be alert for potential sales of sensitive or classified defense articles which would require the release of CMI.

In those instances which would require inter-agency technology security and foreign disclosure (TSFD) release (i.e., when the SCO becomes aware of credible demand signals indicating the probable submission of an LOR for Price and Availability (P&A) or LOA, or a commercial Request for Information or Request for Proposal for such items) the SCO should develop a Pre-LOR Assessment Request (PAR), as directed in SAMM C3.1.2, which will serve in place of a Country Team Assessment (CTA) to inform the inter-agency community and prepare the cognizant Implementing Agency (IA) to initiate TSFD processes for the timely release of information.

When no formal LOR is available, a PAR serves in place of an LOR and CTA as grounds for the IA to initiate applicable foreign disclosure and technology security release processes. However, it should be noted that a PAR does not serve in place of an LOR, or for any purpose other than initiation of the foreign disclosure and technology security release process.

In the preparation of the PAR, the SCO should compile the information described at SAMM Table C3.T2, and consult with the relevant IAs and CCMD for releasability and technical information. When complete, the SCO forwards the PAR to the CCMD. Because the PAR is an extraordinary process, a CCMD endorsement is required in each case to support initiation of the TSFD release processes. The CCMD provides comments on each of the elements addressed in the PAR in the endorsement, and forwards the PAR and endorsement to the Joint Staff, the applicable IA, and DSCA. This process forms the basis for a collaborative effort to analyze the recipient nation's military requirements, in order to identify a capability that fulfills those requirements and initiates DoD's TSFD processes to meet the partner's acquisition needs.

Export Control Reform Initiative

Previously in this chapter, the terms "export reform" and "Export Control Reform Initiative" were introduced. This initiative is a very large and dynamic shift in how the USG makes decisions and manages the export of military items. The changes under export reform are still being written and will take years, perhaps over a decade, to come to fruition. The purpose of this section is to provide familiarization with some aspects of the initiative.

The Four Singularities

On 13 August 2009, President Obama announced the review of the U.S. export control system. In April 2010, then Secretary of Defense Robert Gates described a new order based on four "Singularities:"

1. A single export control licensing agency
2. A unified control list
3. A single primary enforcement coordination agency
4. A single integrated information technology system

The Administration intends to create a single, independent licensing agency with members from the existing Departments of State, Commerce, and Treasury serving as a board of directors. Specific details of how and when the new agency will be created has yet to be announced.

The first step toward the goal of a unified control list is manifest in the mass movement of military items from the DoS USML to the DoC CCL under the new 600 series. Information on the current status of this action can be found under the DoS and DoC sections earlier in this chapter.

The Export Enforcement Control Center (E2C2) has been developed to deconflict investigations, serve as a central contact point for coordinating export control enforcement and synchronize outreach programs. In November 2010, the President signed Executive Order 13558 establishing the "Homeland Security Investigations (HSI) Center," housed under the Department of Homeland Security with representation from the Departments of Commerce, Defense, Energy, Justice, State, Treasury, and the Office of the Director of National Intelligence. The HSI is now the primary forum for enforcement and intelligence agencies to coordinate export enforcement actions.

The fourth singularity is the creation of a single information technology system to be used to administer the export control system. The USXPORTS database, is currently used by the DoD, DoS, DoE, and DoC to track license applications.

Technology Security and Foreign Disclosure (TS&FD) "Pipes"

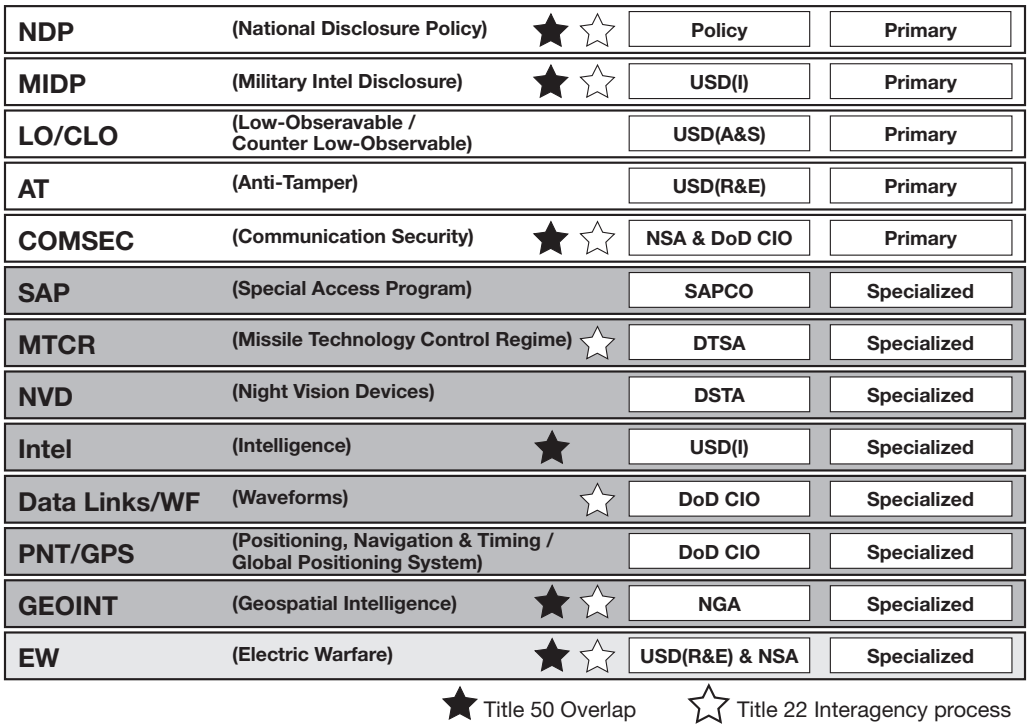
At the core of TS&FD reform is the establishment of policy and responsibilities intended to minimize complexities while ensuring timeliness and efficient processing of disclosure requests. Within the DoD, one of the first export reform adjustments was a codification of those processes and procedures which bear on the approval to export military technology. Previously, it was difficult to discern whether all necessary reviews and decisions were accomplished due to lack of clarity regarding the multitude of processes and approvals potentially necessary for a given export. While different communities within DoD may have been cognizant of the review/approval processes necessary in certain specific areas, there had been no comprehensive documentation of all of potentially applicable procedures. With this in mind, the existing export/foreign disclosure decision-making process was more clearly mapped-out in what has come to be known as the "Thirteen Pipes of Technology Security and Foreign Disclosure," as seen in Figure 7-3. While it is likely that no decision will need to undergo review/approval procedures in all these thirteen pipes, it is now much more likely that individual export/foreign disclosure cases will be more comprehensively planned out in advance, and more easily monitored, so that unexpected delays may be resolved, and faster comprehensive export decisions rendered.

Technology Security and Foreign Disclosure (TS&FD) Review Processes

In January 2010, the Export Control Reform Task Force (ECR TF) issued a report in response to Presidential Study Directive 8 (PSD 8). The report found that the existing DoD-led TS&FD review processes have many strengths and have served DoD well for many years. However, these processes need to be harmonized and streamlined to better serve DoD, our international partners, and national security strategy. The ECR TF ultimately recommended initiation of an effort "to streamline and harmonize" USG TS&FD processes.

The thirteen separate but related TS&FD processes, or "pipes" (see Figure 7-3), support DoD TS&FD release decisions. Additionally, each MILDEP, and many DoD Agencies have internal review processes for approving the transfer of capabilities and technologies within their purview.

Figure 7-3
Thirteen Pipes of Technology Security and Foreign Disclosure

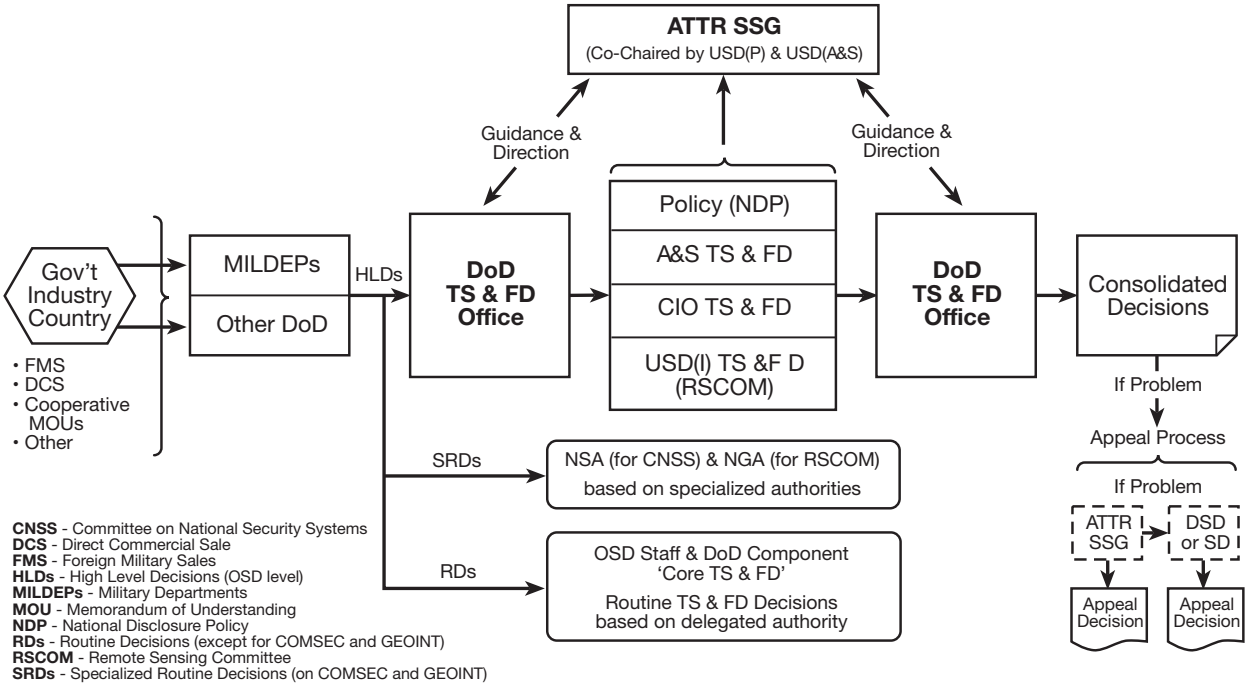


In response to the recommendations outlined in PSD 8, the Deputy Secretary of Defense has further empowered the Arms Transfer and Technology Release Senior Steering Group (ATTR SSG) as the primary forum for review and adjudication of High Level Decision (HLD) TS&FD release requests. Also established was the Technology Security and Foreign Disclosure Office (TSFDO), which is designed to serve as the ATTR SSG's Executive Secretariat. The ATTR SSG has been charged with streamlining and harmonizing DoD TS&FD release processes. The ATTR SSG develops, guides, and directs (consistent with U.S. policy and national security objectives) DoD-wide reform, implementation, and subsequent management of the DoD TS&FD system, and ensures critical U.S. technologies are protected, and release considerations are balanced with building allied and partner nation capability objectives.

The TSFDO facilitates the coordination and synchronization of release requests through the TS&FD processes, with the goal of providing transparency, and timely/well-informed HLDs (See Figure 7-4). Among its many functions, the TSFDO consults with various DoD TS&FD authorities in assessing and recommending changes to the existing TS&FD policies and processes; develops and implements procedures and checklists that provide guidance to the DoD TS&FD community on submission formats for TS&FD HLD requests; and conducts screening, triage, staffing and tracking functions for those HLDs being considered by the ATTR SSG.

Ultimately, all of the above-mentioned reforms are intended to foster the continued growth of a healthy defense industrial base, reduce stresses on U.S. forces, and facilitate efforts in training and equipping forces in countries where doing so advances U.S. national security interests.

Figure 7-4
DoD TS & FD System



False Impressions

It is the policy of the U.S. to avoid creating false impressions of its intention to provide classified military material, technology, or information. Lack of strict adherence to this policy may create problems. Much military hardware is unclassified; however, this same unclassified hardware, if sold, may require the release of classified information for its operation or maintenance, or for the foreign recipient training. Therefore, any disclosure decision must be made based on the classification level of all information which may be required for release if the system were to be transferred. If the proposed foreign recipient is not authorized to receive the highest level of classified information required, no information, not even CUI, may be released or discussed until the required authority is obtained. This means that there can be no weapon specific information, and no release of FMS price and availability (P&A) data until authority is obtained to release the highest level of classified information ultimately required for disclosure.

In order to avoid false impressions, designated disclosure authorities must authorize in advance any proposals to be made to foreign governments that could lead to disclosure of classified military information, technology, or materiel.

Export Approval and License Process

Before discussing the approval and license process for the authorized export of military articles or services, the term "export" must first be defined. To paraphrase the ITAR Section 120.17, an export is the sending or taking defense articles out of the U.S. in any way. This includes transferring registration, ownership, or control of an item on the USML to a foreign person. It also includes disclosing, orally or visually, any information on defense articles to a foreign person, whether in the U.S. or abroad. That means that if you discuss U.S. military technology anywhere with a foreign person and you do not have an authorization to do so, this may well constitute an illegal transfer. This subject is covered in more detail under the "Department of Defense Policy on Technology Transfer" block covered earlier in this chapter.

Part 127 of the ITAR covers violations and penalties of unlawful export, re-export or retransfer or attempt to retransfer of any defense article or technical data for which a license or written approval is required from the DoS.

Licenses for the Export of Defense Articles

The ITAR, primarily Parts 123 and 125, provide the licensing requirements for the permanent and temporary export and import of defense articles and/or services of items on the USML. Any "person" who intends to permanently/temporarily export or import defense articles or services must obtain the approval of the State Department's Directorate of Defense Trade Controls (PM/DDTC) prior to the action unless there is a regulatory exemption. A "person" is defined in the ITAR as, "a natural person as well as a corporation, business association, partnership, society, trust, or any other entity, organization or group, including governmental entities." Export approval usually comes in the form of a license. The four kinds of licenses, Department of State Publication 5 (DSP-5), DSP-85, DSP-73, and DSP-61 (see Table 7-2).

ITAR Section 123.10 states that completed DoS Form DSP-83, provided to DDTC certifies the non-transfer and use assurance certificate required for the export of SME, classified articles, and technical data to a third party. DDTC may also require the completion of a DSP-83 for any other export of defense articles and technical data as it sees fit. A license will not be issued until a completed Form DSP-83 has been received by DDTC. The form is to be executed by the foreign consignee, the foreign end-user, and the applicant which is the U.S. industry vendor that will request the license. Application for export license for the permanent or temporary export or import of classified defense articles and services for DCS must be made on DoS Form DSP-85. Application must be made by a U.S. national in accordance with the provisions of Sections 125.3, 125.7, and 125.9 of the ITAR. Note, DoS has provided guidance to DSCA regarding the requirement for DSP-83 for repair and return. As long as the import and reexport is covered by a valid LOA and DSP94, the DSP 85 is not required for classified repair and return.

Table 7-2 provides a guide for which form is required for the export of munitions list items through either FMS or direct commercial sale.

Export License Applications Staffing within Department of Defense

As stated earlier in this chapter, the License Directorate of DTSA is DoD's entry point for export requests from the DoS and DoC. It is the technical responsibility of this directorate's staff to ensure that the MILDEPs, appropriate DoD agencies, and the technical staff of the USD (A&S) and (R&E) review applicable export requests or munitions cases.

After receiving recommendations from the DoD review, the DTSA License Directorate develops the DoD position in concert with DTSA technical and policy staffs, and forwards the position to the DoS or DoC, respectively.

Table 7-2
Forms to be Used for Export/Import of United States Munitions List Items

Activity	Foreign Military Sales	Commercial Sales
Registration Statement	N/A for gov't shipment	DS-2032
Permanent export of unclassified defense articles and related unclassified technical data	LOA and DSP-94	DSP-5
Permanent/temporary export of classified defense articles and related classified technical data	LOA and DSP-94	DSP-85 (with DSP-83)
Temporary import of classified defense articles and related classified technical data	LOA and DSP-94 (DSP-85 may be required)	DSP-85
Temporary export of unclassified defense articles	N/A	DSP-73
Temporary import of unclassified defense articles	ITAR Exemption 123.4	DSP-61
Non-transfer and use assurances for export of defense articles and services	N/A (Already included in LOA)	DSP-83
Shipper's export declaration	Department of Commerce Form 7525-V	Department of Commerce Form 7525-V

Foreign Military Sales License Exemption

To paraphrase Section 126.6(c) of the ITAR, when using the FMS program, a license from the DoS is not required if the defense article or technical data or a defense service to be transferred was sold, leased, or loaned by the DoD to a foreign country or international organization using the LOA as authorization and the LOA has not expired. In other words, the entire FMS program operates under a licensing exemption authorized by the ITAR. The actual documents required to use this exemption are the DSP-94, "Authority to Export Defense Articles Sold Under the Foreign Military Sales Program," and a copy of the LOA. The ITAR Section 126.6(c)(6)(ii) specifically states, "At the time of shipment, the Port Director of U.S. Customs and Border Protection is provided an original and properly executed DSP-94 accompanied by a copy of the LOA and any other documents required by U.S. Customs and Border Protection (CBP) in carrying out its responsibilities." Prior to DSCA policy letter 18-62, hardcopies of both the LOA and DSP-94 documents were lodged at the primary port of export for items being exported under the LOA. The LOA case identifier was listed on the DSP-94 to correlate it with the specific LOA that authorized the export. The DSP-94 also identified the USML categories of items to be exported and the total value of the military items to be exported under the case. Customs agents would then decrement the value of items being exported on each individual export under the case from the original value listed on the DSP-94. In this way, the customs agents could validate that there was a remaining LOA value for the items that were to be exported. Per DSCA policy letter 18-62, the LOA and DSP-94 information will now be electronically provided to CBP via the Security Cooperation Information Portal (SCIP) in lieu of hardcopy documents.

Commercial Agreements Requiring Approval by Department of State

Besides normal export licenses, when approved by DDTC, the ITAR provides for commercial agreements that give authorization to export certain types of technical information and services. These differ from normal export licenses in that they are typically broader in scope, more flexible, and may remain in effect for longer periods of time. These agreements are typically for ongoing projects rather

than a one-time export. The ITAR recognizes three categories of such agreements:

- Technical assistance agreement (TAA). An agreement for the performance of defense services or the disclosure of technical data, as opposed to an agreement granting right of license to manufacture defense articles [22 CFR 120.22]
- Manufacturing licensing agreement (MLA). An agreement whereby a U.S. person grants a foreign person an authorization or a license to manufacture defense articles abroad and which involves or contemplates the export of technical data or defense articles or the performance of defense services or the use by the foreign person of technical data or defense articles previously exported by the U.S. person [22 CFR 120.21]
- Distribution agreement. A contract between a U.S. person and a foreign person to export unclassified defense articles to a warehouse or distribution point outside the U.S. for subsequent resale. These agreements contain conditions for special distribution, end-use and reporting [22 CFR 120.23]

As a review, there are three authorized methods to export USML items to a foreign government or international organizations.

1. An export license
2. An export agreement
3. An ITAR exemption (i.e., ITAR 126.6(c), FMS use of an LOA and DSP-94)

International Programs Security Requirements (ISPR)

International Visits and Assignments

DoDD 5230.20, *Visits and Assignments of Foreign Nationals*, sets forth standard procedures concerning requests for visits, certification of liaison officers and personnel exchange programs. SAMM, Section C3.4, "Visits, Assignments, and Exchanges of Foreign Nationals," provides further discussion relating to SC.

Foreign representatives (i.e., foreign nationals or U.S. citizens or nationals who are acting as representatives of a foreign government, firm, or person) may be authorized to visit DoD components or U.S. defense contractor facilities only when the proposed visit is in support of an actual or potential USG program (e.g., FMS, USG contract, or international agreement). The DoD and U.S. defense contractors receive over 230,000 foreign visitors annually on matters related to mutual security and cooperation. These visits play a vital part in the exchange of information and technology as a part of U.S. international commitments. These visits account for more transfer of CMI and CUI than all other transfer mechanisms combined.

International Visits Program

The International Visits Program (IVP) establishes policy and procedures to control international visits, and the information to be transferred during those visits. DoD policies and procedures pertaining to foreign visits are designed to achieve three objectives.

- Facilitate planning, scheduling, and administration of a visit
- Provide a vehicle for consideration of proposed export/disclosure decisions related to the visit and record the decision(s)
- Obtain the required assurances regarding the security clearance, need-to-know, and sponsorship from the visitor's government if classified military information is involved

Types of Visits

Under the IVP, there are three types of visits that may be authorized:

- One-time—a visit normally less than thirty days
- Recurring—recurring visits over a period of time; normally not exceeding one year
- Extended—visit for an extended period of time, e.g., certifications of liaison officers; normally up to one year or term of contract or applicable export license

In an emergency, a one-time visit may be submitted for approval less than twenty-one working days before the visit start date. Emergency visits may only be authorized if failure to make the visit would jeopardize performance on a contract or program, or cause the loss of a contract opportunity. These authorities may not be used to employ foreign nationals.

A visit can be considered a "hosted visit" when a DoD official or entity extends an invitation to a foreign national or delegation. Whether DoD funds any portion of the visit is an entirely separate issue from the approval of the visit under the IVP. Before issuing an invitation, DoD officials must ensure that any classified information proposed for disclosure is approved by the delegated disclosure authority. DoD officials who wish to invite foreign representatives to visit a DoD component, or who wish to have a foreign national certified to the component, shall coordinate their actions with the Defense Intelligence Agency (DIA) or the MILDEP concerned, before extending an invitation. Amendments to visits may be used only to change dates (no earlier dates) and list of visitors. The information to be discussed during the visit cannot change.

Visit Procedures

The DIA coordinates the IVP for DoD. Visit requests to DoD organizations or facilities are submitted by the foreign embassy in Washington DC, usually by a military attaché of the partner nation. The requests normally are submitted electronically through the automated Foreign Visit System (FVS), which has been provided by DIA to foreign embassies. The FVS is a component of the Security Policy Automation Network (SPAN). Requests by foreign embassies shall normally be submitted at least thirty days in advance for visits and ninety days in advance for liaison officer certifications.

The FVS automatically routes each request for visit to the Defense Visit Office (DVO) in one of four designated organizations. These include the Department of the Army, Department of the Navy, and Department of the Air Force for all organizations, facilities, and other entities under their control. The fourth organization is DIA itself, which administers visit requests for the Office of the Secretary of Defense, the Joint Staff, defense agencies, and their contractors. The DVOs forward, as necessary, the visit requests to the appropriate foreign disclosure offices of the organizations to be visited, and seek their comment. Based on this input, the DVO renders a decision on the visit, which is returned over the same electronic path used for submission to the embassy of the country submitting the visit request. There are three possible responses to a visit request through IVP channels:

- Approved—The visit can occur and the specified information can be disclosed
- Denied—The visit can occur but the specified information cannot be disclosed
- Not sponsored—There is no apparent government program. The visit can occur and information can be disclosed if there is a license or other authorization

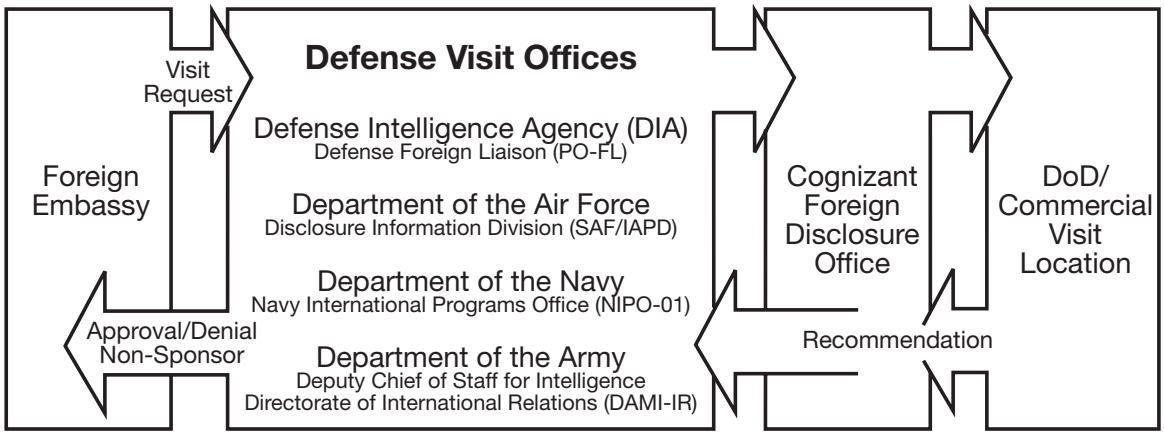
Notification of approval of a foreign request for a visit or certification to a DoD component shall be forwarded to the contact officer of the DoD component concerned, or where the representative will visit. This notification shall contain adequate guidance regarding the parameters of the subject visit

and the maximum permissible level of classified information that has been authorized for disclosure. Correspondence with DoD contractors relative to approved foreign visits shall be forwarded to the cognizant DSS regional office for transmittal to the contractor.

Disclosures of classified information to foreign visitors and certified foreign representatives shall be limited to releasable oral and visual information, unless the release of documentary information is specifically authorized in an approved visit request or letter of acceptance for certified officials, or when the U.S. contractor has secured an export license specific to the documentation intended for release. When documentary release is authorized, the visitor must have courier orders.

Figure 7-5 provides an overview of the IVP within DoD. At any time, participating activities have immediate access to all visit request status information.

Figure 7-5
International Visit Program



A request of visit authorization is not required at a contractor facility when the information to be disclosed is unclassified and (1) it is not subject to export controls, or (2) it is subject to export controls, but a contractor has an export license. A visit authorization is typically not required at a DoD facility when the facility is open to the public and the information is open for public release according to service regulations.

However, if classified information is to be disclosed, a visit request must be submitted even though the contractor has a valid export authorization or license. In this case, the visit request is used to pass the security assurance on the visitors. Requests for classified documentary information resulting from a foreign visit shall otherwise be processed through normal foreign disclosure channels. In either case, classified documentary information shall be transferred through government-to-government channels, unless the visitor is also acting as a courier and has courier orders.

Role of Security Cooperation Offices in International Visits

SCO personnel should be cognizant of the official travel of both host nation personnel to DoD organizations, as well as the travel of DoD personnel into country. SCOs frequently coordinate visits by host nation personnel to destinations such as a combatant command headquarters or a MILDEP installation for a program management review. However, the SCO cannot submit the visit request, which must originate in the host nation embassy in Washington DC through the FVS. SCOs remind their host nation counterparts of this requirement and note that their own assistance in scheduling a visit is dependent on formal approval through the FVS. A SCO cannot approve a visit to any DoD organization or facility, other than its own office.

For DoD visitors traveling into the host nation, the SCO should control these through the granting or denying of country clearance. In doing this, the SCO follows the procedures in DoD 4500.54, *DoD Foreign Clearance Guide*. The SCO may also support DoD visitors by passing assurances and other documentation to and from the host nation, and by using its office as necessary to appropriately store CMI or CUI.

Defense Personnel Exchange Program

The Defense Personnel Exchange Program (DPEP) authorizes the exchange of personnel between the U.S. military services and their counterparts of friendly governments for assignment to established positions within the military services. This exchange is implemented under an agreement conforming to DoDD 5530.3, *International Agreements*. Assignments can be negotiated as a reciprocal exchange of military personnel. Also, civilian position assignments such as intelligence analysts, scientists and engineers, medical personnel, and administrative specialists may be negotiated. Exchange personnel perform the functions of the specific position within the organization to which they are assigned. Since they are not designated officials of their government, classified information may not be released into their permanent custody. They may only be given oral or visual access to specific classified information authorized in the applicable delegation of disclosure authority letter (DDL). Written procedures must be developed to prevent inadvertent disclosure of classified or CUI as described in DoDD 5230.20. DPEP assignees may not act as a representative of their government.

Foreign Attendance at Classified Meetings Leading to Contract Opportunities

The USG has entered into cooperative agreements with allies and other friendly nations that allow the exchange of information in specific areas of mutual interest required for their participation in contractual opportunities (see Chapter 13 for a discussion of reciprocal procurement memoranda of understanding). Planning for meetings that may lead to contracts for foreign nationals shall be based on the assumption that there will be foreign attendance.

Visits Overseas by Department of Defense Personnel

The policy for overseas travel of DoD personnel is covered under DoDD 4500.54E, *DoD Foreign Clearance Program* (FCP), the *DoD Foreign Clearance Manual* (FCM), and *Foreign Clearance Guide* (FCG). The FCM and FCG implement clearances and DoD personnel travel clearances through U.S. embassies for overseas travel. Normally, thirty days advance notice is needed before travel. Procedures also must be established to ensure disclosure authorization has been obtained if classified or export controlled unclassified information is to be divulged. A "theater clearance" is required for visits to a U.S. military facility overseas, as specified in the FCG. A "country clearance" is required for visits to a host government organization or contractor facility.

International Transportation of Classified Military Material

To ensure government accountability and control are maintained for classified material, all international transfers take place through official government-to-government channels or other channels mutually agreed upon in writing by the sending and receiving governments (i.e., collectively, a government-to-government transfer), consistent with the government-to-government principle. Transfers must take place between Designated Government Representatives (DGRs) who are appointed by their governments or international organizations. The U.S. DGR for Direct Commercial Sales (DCS) is a Defense Security Service (DSS) representative. Another USG employee at a facility may be given this responsibility. The U.S. DGR is responsible for performing the "foreign disclosure" verification (i.e., verifying the classified material to be transferred is covered by an export authorization); ensuring appropriate written security arrangements are in place; and decrementing and endorsing the license back to DDTC. In cases when a DSS, or other USG official is not immediately available, DSS may

delegate certain DGR functions to a company's Empowered Official or Facility Security Officer. However, DSS must ensure that the proper documentation is in place before delegating such authority, must maintain oversight responsibility, and must follow-up to ensure that proper procedures were followed. For FMS shipments, the U.S. DGR is appointed by the FMS case implementing agency.

The DGR of the recipient government or international organization receives or verifies receipt of the information or material (depending on the location of the transfer and the arrangements specified in the LOA and/or contract and the transfer plan) on behalf of the recipient government or organization.

The official transfer of security responsibility is not complete until the foreign government's DGR notifies the U.S. DGR that the recipient government or organization has taken final custody of the classified material and assumed full control for its safeguarding under bilateral security or program specific security agreements between the USG and the foreign government. A freight forwarder or commercial carrier is a transfer agent and cannot be a DGR. All transfers must be consistent with the NISPOM for commercial sales and DoDM 5200.01 and the SAMM Chapter 7 for FMS sales.

Defense Security Service Role in International Programs

A role of the Defense Security Service (DSS) is to provide government contracting agencies with an assurance that U.S. defense contractors are both eligible to access and properly safeguard any classified information. In fulfilling this obligation, DSS administers the National Industrial Security Program (NISP) operating on behalf of USD (I). DSS does not develop industrial security policy. DSS implements industrial security policy established by USD (I) for international programs executed by USD (P).

Facility Security Clearance

Prior to a defense contractor being granted access to classified information, the contractor must be sponsored for a facility security clearance (FSC). This sponsorship is based upon a *bona fide* procurement need, and is submitted to DSS by a U.S. or foreign government contracting activity or by another contractor already cleared under the NISP. DSS will conduct a facility clearance survey to determine the contractor's eligibility for access to classified information, and will review the contractor's organizational structure and key management personnel, and adjudicate any existing foreign ownership, control, or influence (FOCI). Once a favorable determination is made and a facility clearance is granted, the contractor will execute a security agreement with the USG. The security agreement is a legal contract to abide by the DoD 5220.22-M, *National Industrial Security Program Operating Manual* (NISPOM). The NISPOM is a contractually binding document and mandates industrial security practices for contractors. The NISPOM derives its authority from the ITAR and implements applicable statutes, executive orders, national directives, and international treaties toward the protection of classified information.

The DSS verifies the export of classified articles and technical data against the license or the U.S. company's empowered official's certification, assures that secure means of transfer have been arranged, and endorses the license back to the DoS. DSS oversees plant visits by foreign nationals and ensures that companies have adequate technology control plans in place for long-term foreign national visitors, foreign national employees, and for FOCI situations. DSS ensures appropriate transportation plans are in place for commercial overseas shipments of classified material and approves contractor international hand carriage arrangements. Additionally, DSS provides security assurances to other governments for U.S. contractor facilities and personnel, and obtains assurances on foreign facilities and personnel. It advises cleared contractors concerning program protection plans, ensures compliance, and trains DoD and contractor personnel on program protection planning. The DSS provides support to cleared contractors operating overseas, and monitors their compliance with the NISPOM. Finally, DSS provides counterintelligence (CI) support to cleared contractors, including CI awareness briefings. More information about DSS can be found at its website: http://www.dss.mil.

Technology Control Plan

The technology control plan (TCP) provides guidance for controlling access to classified and unclassified export controlled information by foreign employees and long-term foreign national visitors of a cleared U.S. contractor's facility. The TCP explains how the requirements of the ITAR, the EAR, and the NISPOM will be carried out. The TCP is developed by the U.S. contractor, based on the requirements of the ITAR, Section 126.13c, and the NISPOM. The content regarding information access and restrictions may be derived from other documents provided by the USG (for example, the license provisos and the program security instructions or the form DD 254, *Contract Security Classification Specification*). The DSS will assist the contractor in developing the TCP and will approve it. A specific TCP may not be required if the company's internal security operating procedures, e.g., standard practice procedures (SPP) contain the necessary details. If security requirements are partially contained in a document such as an SPP and additional export control procedures are in a TCP, the latter must refer to the applicable portions of the other document.

DoD Central Adjudicative Facility (CAF)

The National Industrial Security Program (NISP) establishes procedures for safeguarding classified defense information that is entrusted to contractors. Included in these procedures is a system for determining the eligibility of industrial personnel for access to classified defense information. The Central Adjudication Facility (CAF) is responsible, on behalf of the Department of Defense (DoD) and twenty-three other departments and agencies, for:

- Determining the personnel clearance eligibility of employees for access to classified information, foreign or domestic
- Maintenance of personnel clearance records and furnishing information to authorized activities
- Processing security assurances, clearances and visits involving the United States and foreign countries
- Monitoring the contractor's continued eligibility in the NISP

Foreign Government and North Atlantic Treaty Organization Information

Foreign Government Information

Foreign government information (FGI) is information that has been provided by a foreign government or international organization, or jointly produced, with the expectation that the information will be treated "in confidence." The information may be classified or unclassified. In addition to TOP SECRET, SECRET, and CONFIDENTIAL, many foreign governments have a fourth level of security classification, RESTRICTED, as well as CUI that is provided in confidence.

As a result of numerous international security and program agreements, the NATO security agreements obligate member nations to adopt common standards of protection. U.S. national policy affords FGI a degree of protection equivalent to that provided to it by the originating government or international organization. Since foreign government accountability and control measures often exceed those of the U.S., the U.S. applies separate security procedures to protect FGI. Because most exchanges are with NATO and its members, the NATO standards are used as the baseline for U.S. procedures for protecting FGI.

FGI, including RESTRICTED and foreign government CUI, must be controlled and managed under E.O. 13526 in order to receive protection equivalent to that provided by the originating government or organization, as stipulated in E.O. 13526 and international agreements. FGI that is classified by the

originating government or organization will be marked with the equivalent U.S. classification, if it is not already marked in English, and the identity of the originating government or organization. Foreign government RESTRICTED and CUI are to be marked, "Handle as CONFIDENTIAL–Modified Handling Authorized." FGI cannot be provided to third country entities or used for a purpose other than that for which it was provided without the consent of the originating government or organization. It must receive protection commensurate with that provided by the originating government or organization. The procedures for handling FGI are contained in two national policy documents, E.O.13526, the Presidential directive on safeguarding classified national security information, and DoD-M 5200.01.

Basic handling procedures for FGI are as follows:

- Storage. The same as U.S. information of the same classification, but FGI is to be stored separately. FGI that is marked "Handle as CONFIDENTIAL–Modified Handling Authorized" is stored in the same manner as U.S. CUI, e.g., in a locked desk or file cabinet.
- Access. Using the need-to-know principle, no access by third country persons without the prior consent of the originating country or organization.
- Transmission. The same as U.S. classified information of the same classification level; however, express commercial carriers cannot be used. Receipts are required for international transfers wherever they occur, although exceptions are made for RESTRICTED information. There are no receipts for CUI.
- Records. TOP SECRET–receipt, dispatch, internal distribution, annual inventory, and destruction (two persons); SECRET–receipt, dispatch, internal distribution, and destruction; CONFIDENTIAL–receipt and dispatch, and as required by originator.

North Atlantic Treaty Organization Disclosure Security Procedures

Basic security requirements are necessary to comply with the procedures established by the U.S. Security Authority for the North Atlantic Treaty Organization Affairs (USSAN) for safeguarding NATO information involved in international programs. DoDD 5100.55 *USSAN Affairs* contains the terms of reference designating the Secretary of Defense as the USSAN for the USG. These requirements are consistent with USSAN Instruction 1-70 and implemented by DoDD 5100.55, and the NISPOM. These documents must be consulted for specific details.

Classification Levels

"NATO information" is information that is circulated within NATO. NATO security regulations prescribe four levels of security classification, COSMIC TOP SECRET (CTS), NATO SECRET (NS), NATO CONFIDENTIAL (NC), and NATO RESTRICTED (NR). The terms COSMIC and NATO indicate that the material is "NATO Information." Another marking, ATOMAL, is applied to U.S. RESTRICTED DATA or FORMERLY RESTRICTED DATA and United Kingdom atomic information released to NATO. Once disclosed to NATO, the classified information loses its country of origin identity and is marked as NATO information. Thereafter, access, dissemination, and safeguarding of the information is accomplished in accordance with NATO procedures. The information remains the property of the provider or originator. Once NATO no longer needs the information, the NATO markings are removed and the information is returned to the originator.

Access Requirements

DoD and contractor employees may have access to NATO classified information only when access is required in support of a U.S. or NATO program that requires such access (i.e., need-to-know).

Access to NATO classified information requires a final DoD personnel clearance (except for RESTRICTED) at the equivalent level and a NATO-specific security briefing discussed later in this chapter. A personnel security clearance is not required for access to NATO RESTRICTED information.

Foreign nationals from nations not members of NATO may have access to NATO classified information only with the consent of the originating NATO member nation or civil or military body. Requests with complete justification, as described in the NISPOM, will be submitted through the cognizant security office (CSO).

Disclosure Briefings

Prior to having access to NATO classified information, contractor and government personnel must be provided a NATO security briefing. The contractor's facilities security officer (FSO) will initially be briefed by the CSO. Annual refresher briefings will be conducted. When access to NATO classified information is no longer required, personnel will be debriefed, as applicable, and acknowledge their responsibility for safeguarding the NATO information.

Marking and Handling NATO Documents

Normally, NATO documents do not carry portion markings as are required for U.S. classified documents. Nevertheless, all classified documents created by U.S. contractors and DoD components will be portion-marked.

NATO classified documents, and NATO information in other documents, may not be declassified or downgraded without the prior written consent of the originating NATO member nation civil or military body. Recommendations concerning the declassification or downgrading of NATO classified information are to be forwarded to the central U.S. registry (CUSR) via the CSO by contractors and via command or organizational channels by government personnel.

NATO classified documents, except for NATO RESTRICTED, are to be stored as prescribed in DoDD 5100.55 and the NISPOM for U.S. documents of an equivalent classification level. However, NATO documents must not be comingled with U.S. or other documents. NATO restricted documents may be stored in locking filing cabinets, book cases, desks, other similar locked containers that will deter unauthorized access, or in a locked room to which access is controlled.

International Transmission of Classified NATO Documents

NATO policy requires the establishment of a central registry for the control of the receipt and distribution of NATO documents within each NATO member country. The CUSR, located in Washington, DC, establishes sub-registries at USG organizations for further distribution and control of NATO documents. Sub-registries may establish control points and sub-control points, as needed, within their activities for distribution and control of NATO documents. COSMIC TOP SECRET, NATO SECRET and all ATOMAL documents must be transferred through the registry system.

Marking the Documents

When a document containing U.S. classified information is being specifically prepared for NATO, the appropriate NATO classification markings will be applied to the document only after the U.S. information contained in the document is authorized for release to NATO.

Multinational Industrial Security Working Group Documents

The multinational industrial security working group (MISWG) is composed of the NATO countries (minus Iceland) as well as Austria, Sweden, Switzerland and Finland. This ad hoc group was organized to rationalize different security practices and develop standard procedures for multinational programs. Although initially developed to standardize procedures among NATO member nations working

jointly on a non-NATO project, the MISWG documents contain procedures that may be used in any bilateral or multilateral program or project, including NATO projects. NATO, NATO countries, and other countries have adopted the MISWG procedures. Therefore, they should be used as the baseline in preparing individual arrangements or when consolidated in a program security instruction (PSI), MISWG Document 5, for international programs.

Most of the MISWG documents provide procedural guidance for implementing security requirements for international programs. Other MISWG documents are used in preparing the content of international agreements and contracts involving access to classified information. The DSS may approve the use of the documents in individual commercial programs. However, the Designated Security Authority, part of DTSA, will approve the use of the documents when they are required by an international agreement such as in a PSI.

More information on the MISWG documents can be found in Chapter 9 of the *International Programs Security Handbook*.

Committee on Foreign Investment in the United States and Foreign Ownership, Control or Influence

Committee on Foreign Investment in the United States (CFIUS)

The Exon-Florio Amendment to the Omnibus Trade and Competitiveness Act of 1988, as amended by the Defense Authorization Act for Fiscal Year 1993, empowers the President to suspend, prohibit or dissolve ("block") foreign acquisitions, mergers and takeovers of U.S. companies. The President has broad authority to block a transaction under the statute if he determines the foreign interest acquiring control might take action that threatens to impair the national security. To exercise his authority, the President must find that:

- There is credible evidence that leads him to believe that a foreign interest might take action to threaten or impair national security.
- Provisions of law, other than Exon-Florio and the Emergency Economics Powers Act, are not adequate to protect the national security.

There is no mandatory requirement for a company to report under the law. Nevertheless, the President or his designee may investigate a merger, acquisition, or takeover at any time, including after a transaction has been concluded. The President can reopen a case on the basis of material omissions or material misstatements in the original notice.

The President delegated responsibility for carrying out the requirements of Exon-Florio to the interagency CFIUS. The CFIUS is comprised of representatives of the Departments of Treasury (chair), Defense, State, Energy, Justice, Homeland Security, Commerce, the U.S. Trade Representative, and the Office of Science and Technology Policy. Membership may also include the heads of any other executive department, agency, or office as the President determines appropriate on a case-by-case basis.

Once CFIUS considers a possible transaction as the result of a notification by the investors, on its own initiative, or at the request of a third party, it has thirty days to decide whether to initiate an investigation. The investigation must be completed no later than forty-five days after its commencement, at which time the committee must present a recommendation to the President. The President is required to render a decision within fifteen days after completion of the investigation. If the President decides to take action as the result of a CFIUS investigation, he must submit a written report to Congress on the actions that he intends to take, including detailed rationale for his findings. The Committee or a lead agency of the Committee may, on behalf of the Committee, negotiate, enter into or impose and enforce any agreement or condition with any party to the specified transaction in order to mitigate any threat to the national security of the U.S. that may arise as a result of the transaction.

Foreign Ownership, Control or Influence (FOCI)

It is not in the interest of the U.S. to permit foreign investment in the defense industrial base where it is inconsistent with U.S. national security interests. USG contracts requiring access to classified information may be awarded to companies under FOCI when adequate safeguards exist to protect national security interests. Within the context of the DoD, national security interests are represented by information and technical data inherent in the development and production of military systems, such as system capabilities and vulnerabilities. If this knowledge is lost or compromised, potential adversaries of the U.S. would have the capability to duplicate or neutralize those systems. As a result, the U.S. must take steps to ensure that foreign interests do not have the power to direct or decide matters for a company operating under a facility security clearance if such power may result in the unauthorized disclosure of classified and CUI, or may adversely affect the award or performance of classified contracts. FOCI encompasses the possible avenues from which unauthorized foreign power may be exerted. When competent authority determines foreign interests have the power to exert such power, measures must be established to negate the FOCI or mitigate the associated risk.

When a company performing classified work is to be acquired by or merged with a foreign interest, an industrial security review is undertaken. The purpose of the review is to determine whether existing industrial security measures require enhancement. The matter of FOCI is considered in the aggregate, and the fact that FOCI elements are present will not necessarily bar a company from receiving a facility security clearance. There are many components of foreign involvement requiring examination to determine whether a company is under FOCI and the extent of FOCI, such as those identified on Standard Form (SF) 328, *Certification Pertaining to Foreign Interest*. Documents other than the SF 328 are analyzed, to include filings with the Security and Exchange Commission for publicly traded companies, articles of incorporation, by-laws, loan and shareholder agreements, and other documents pertinent to potential foreign control or influence.

The FOCI is then examined within the context of risk factors such as the foreign intelligence threat, potential for unauthorized technology transfer, record of compliance with laws, regulations, and contracts, and the nature of applicable international agreements between the U.S. and foreign governments. If a company is determined to be under FOCI, and risks associated with FOCI are considered unacceptable, the company would be ineligible for a facility clearance or an existing clearance would be suspended or revoked, unless steps are taken to negate FOCI or mitigate associated risks to the satisfaction of the USG. The principal objective of each arrangement is to ensure there is no unauthorized access to classified and CUI by foreign owners, their agents or representatives, or by other non-ownership derived sources of foreign control or influence. For a detailed discussion of these arrangements and agreements, refer to Chapter 12 of the *International Programs Security Handbook* and the NISPOM.

SUMMARY

The DoD has identified the areas where U.S.-origin technology and other sensitive information should be rigidly protected. These include the critical military technology products, transfer mechanisms and information which DoD has determined should be subject to export and disclosure controls. The NDP provides guidance on the disclosure and release of U.S. classified military information. The criteria for disclosure decisions in the NDP-1 and NSDM 119 do not categorically dictate whether classified military information will be released to a specific country. These decisions are made on a case-by-case basis, in accordance with satisfying all of the five policy objectives of NSDM 119, which are restated in DoDD 5230.11.

Controlling the transfer of selected technologies is but one way to maintain the integrity of the U.S. defense-related industrial base. However, the extent of control is at issue. Many feel that controls should be tempered by the realities associated with worldwide competition and the impacts upon U.S.

industry and the preservation of U.S. economic security as the prerequisite condition to maintaining national security. Technology transfer issues continue to play an important role in government-to-government sales programs, commercial sales programs, international armaments cooperation programs, and industrial base considerations.

Policies and supporting directives governing technology transfer emphasize the application of the U.S. policy and legal requirements in the AECA, E.O.13526, NSDM 119, NDP-1, and DODD 5230.11 to each case, and the analysis of a potential recipient's need, the intended use and protection measures for such information. The directives are explicit as to procedures and channels to be followed to preclude unwarranted release and disclosure of information.

References

Laws

Arms Export Control Act

Atomic Energy Act of 1954

Defense Authorization Act of 1986 (Nunn Amendment/NATO Cooperative R&D)

Defense Authorization Act of 1993, Defense Technology and Industrial Base Reinvestment and Concession

Energy Reorganization Act of 1974

Export Administration Act of 1979

Freedom of Information Act

Public Law (PL-110-49), 26 July 2007, Foreign Investment and National Security Act of 2007.

Stephenson-Wydler Technology Innovation Act of 1980

Department of State Documents

DDTC Website: http://www.pmdtc.state.gov/regulations_laws/itar.htn

International Traffic and Arms Regulations (ITAR) (22 CFR 120-130).

Department of Defense Documents

DoD 4500.54E, *DoD Foreign Clearance Program*.

DoD 5220.22-M, *National Industrial Security Programs Operating Manual* (NISPOM).

DoD-M 5200.01 *DoD Information Security Program*.

DoDD 5100.55, United States Security Authority for North Atlantic Treaty Organization Affairs.

DoDD 5230.9, *Clearance of DoD Information for Public Release*.

DoDD 5230.11, *National Policy and Procedures for Disclosure of Classified Military Information to Foreign Governments and International Organizations*.

DoDD 5230.20, *Visits and Assignments of Foreign Nationals*.

DoDD 5230.24, *Distribution Statements on Technical Documents*.

DoDD 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*.

DoDD 5400.07, *Freedom of Information Program (FOIA)*.

DoDI 2040.02, *International Transfer of Technology, Articles, and Services*.

DSCA Manual 5105.38-M, *Security Assistance Management Manual* (SAMM), Chapter 3. http://www.samm.dsca.mil/.

U.S. Security Authority for the North Atlantic Treaty Organization, Instruction I-07.

Other U.S. Government Documents

Defense Technical Information Centers (DTIC). www.dtic.mil

Executive Order 13526.

National Security Decision Memorandum 119.

Other

Bandarian Security Cooperation Sample Case Documents

Congressional Research Service, Report to Congress, "The U.S. Export Control System and the President's Reform Initiative," dated January 13, 2014.

International Programs Security Handbook. http://www.discs.dsca.mil/_/pages/resources/default.aspx?section=publications&type=ips

Attachment 7-1
National Disclosure Policy Committee Members

National Disclosure Policy Committee Members

General Members are representatives of:

Secretary of State

Secretary of Defense (appoints Chairman)

Secretary of the Army

Secretary of the Navy

Secretary of the Air Force

Chairman, Joint Chiefs of Staff

The Special Members are representatives of:

Secretary of Energy

Director of National Intelligence

Under Secretary of Defense for Policy

Under Secretary of Defense for Acquisition, and Sustainment

Under Secretary of Defense for Intelligence

Assistant Secretary of Defense for Networks and Information Integration

Assistant to the Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs

Director, Defense Intelligence Agency

Director, Missile Defense Agency

Director, National Geospatial-Intelligence Agency

Director, National Security Agency

Attachment 7-2
National Military Intelligence Disclosure Policy Committee Members

Members will serve as representatives of:

The Secretary of State

The Secretary of Defense

The Director of National Intelligence

The Secretary of the Army

The Secretary of the Navy

The Secretary of the Air Force

The Under Secretary of Defense for Policy

The Chairman, Joint Chiefs of Staff

The Director, Central Intelligence Agency

The Director, National Security Agency

Director, Defense Intelligence Agency

Director, National Geospatial Intelligence Agency